Julia Giebultowicz

July 28, 2011

Instruction and Technology

Safe and Responsible Internet Use

1. Based on the information provided in the websites what **Internet safety rules** would you teach upper elementary and middle school students? Consider issues of privacy, safety from predators, inappropriate content, and digital etiquette.

Outside of the control I have to limit kids' computer usage, for example creating filters, I would teach students to not go to websites that they do not already know, especially if it doesn’t end in .org, .gov, or .edu, and to ask an adult before they want to explore a new website. I would teach them to NEVER interact with anyone they do not know in person, and would generally discourage them from social networking until they are older. I would encourage an open dialogue about what they were doing on the internet.   
  
2. Based on the information provided in the websites what safety procedures would you teach older students about **social networking**? Consider issues of privacy, inappropriate content, safety, and digital etiquette.

I think it would be a good idea to have some sort of workshop on safe Facebook uses with students. I would have an in depth discussion with students about what they think they should use Facebook for. I would give detailed instructions on how to modify the privacy settings on students' Facebook pages; they can be very complicated. As a guide, perhaps I would use the “How to Optimize Facebook Settings for Young People” section of “A Parent's Guide to Facebook” at [safekids.com](http://safekids.com" \t "_blank). It claims to protect children in terms of safety, privacy, and reputation. I would clearly explain the risks of being too open and public on your Facebook page. For people under 18, Facebook will not allow incoming messages from people who are not friends or friends of friends. I would make sure all students were honest about their age. I would follow the same procedures for other social networking sites such as twitter or MySpace, of course.

3. Based on the information provided in the websites what safety procedures would you teach middle and high school students about **cyber bullying**? Include the definition of cyber bullying, how to prevent bullying, and what the victim should do.

Cyber bullying is “bullying through Internet applications and technologies such as instant messaging (IM), social networking sites, and cell phones.” I would teach students to keep their social networking sites very private, and their passwords completely secret. This will prevent people from posting unwanted/hurtful things on their site or entering their profiles without permission. I would teach children to take the high road and not to respond or retaliate if the receive a hurtful comment; this will only make things worse. I would also bring awareness to how innocent actions can have devastating results, and that just because something happens in cyber space, doesn’t mean it doesn’t hurt as much as if it had happened in person. This video would be a good example of an action that resulted in unintended cyber bullying: [www.netsmartz.org/RealLifeStories/CantTakeItBack](http://www.netsmartz.org/RealLifeStories/CantTakeItBack). I would teach students that if they are victims, they should save the evidence and talk to a trusted adult or close friend right away, and block the bully.   
  
4. Based on the information provided in the websites what safety procedures would you teach older students about **sexting**? Consider the definition of sexting, possible consequences for the person who sends sexual messages, and how to report sexually inappropriate content.

According to netsmartz.org, sexting is “the exchange of sexually suggestive or nude images between minors via cell phone.” I would make sure students were very aware of the *legal* as well as *emotional* consequences of sexting. I would tell them to remember that someone who is their boyfriend today will probably not be their boyfriend forever… but they’ll still have those pictures on their cell phones! The distribution of those pictures could result in embarrassment, negatively effecting one’s reputation, or even problems with the law (due to child pornography laws.) I would let students know that if they receive this content, they should talk to a trusted adult, and if it is inappropriate or offensive, to report it to [www.cybertipline.com](http://www.cybertipline.com/" \t "_blank) or law enforcement.   
  
5. Based on the information provided in the websites what safety procedures would you teach middle and high school students about **cyber security**? Consider the dangers from hackers, viruses, and spyware and precautions students can take to avoid these dangers.

I would tell children to NEVER provide any personal data to any website they do not know, especially their e-mail address, physical address, or phone number. Ask an adult first. I would also tell them to ask an adult before downloading any software or files in case there may be viruses. If they want to buy something online, an adult of course would have to be present and approve the website. I would inform them of the consequences of having their computer hacked, getting a virus, or having their identity stolen.